ABSTRACT OF THE DISCLOSURE

Methods for providing and extracting hidden information in firmware images using steganographic processes. Information is hidden in binary firmware images, such as drivers, using a steganographic process in which the functionality of the binaries do not change, and the size is not increased. During a pre-boot phase of a computer system, binary firmware drivers containing hidden steganographic data are identified, and a steganographic extraction process is performed to extract the hidden data. In one embodiment, a hash is employed on an authentic binary image to uniquely identify the op code content. The digest from the hash is stored in the steganographic data. In one embodiment, a vendor's private key and optional signature is used to encrypt the hash. A similar hash is performed on the binary image of a discovered binary firmware driver, and the authentic hash digest is extracted from the steganographic data. The hash digests are compared to authenticate the binary firmware driver.